Настройте аномальное обнаружение оконечной точки и осуществление на ISE 2.2

Содержание

Введение

Этот документ описывает Аномальное Обнаружение Оконечной точки и Осуществление. Это - новая Копировальная функция, представленная в платформе Cisco Identity Services Engine (ISE) для расширенной сетевой видимости.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Проводная конфигурация Обхода проверки подлинности MAC (MAB) на коммутаторе
- Беспроводная конфигурация MAB на Контроллере беспроводной локальной сети (WLC)
- Конфигурация изменения авторизации (CoA) на обоих устройствах

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

1. Платформа Identity Services Engine 2.2

2. Контроллер беспроводной локальной сети 8.0.100.0
3. Коммутатор Cisco Catalyst 3750 15.2 (3) E2
4. Windows 10 с проводным и беспроводными адаптерами

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

ISE может обнаружить оконечные точки, которые вовлечены в спуфинг MAC-адреса. Как только это было обнаружено, ISE может принять меры (с CoA) и принудить определенную политику для ограничения доступа подозрительной оконечной точки.

Как только обнаружение включено, ISE контролирует любую новую информацию, полученную для существующих оконечных точек и проверок, если изменились эти атрибуты:

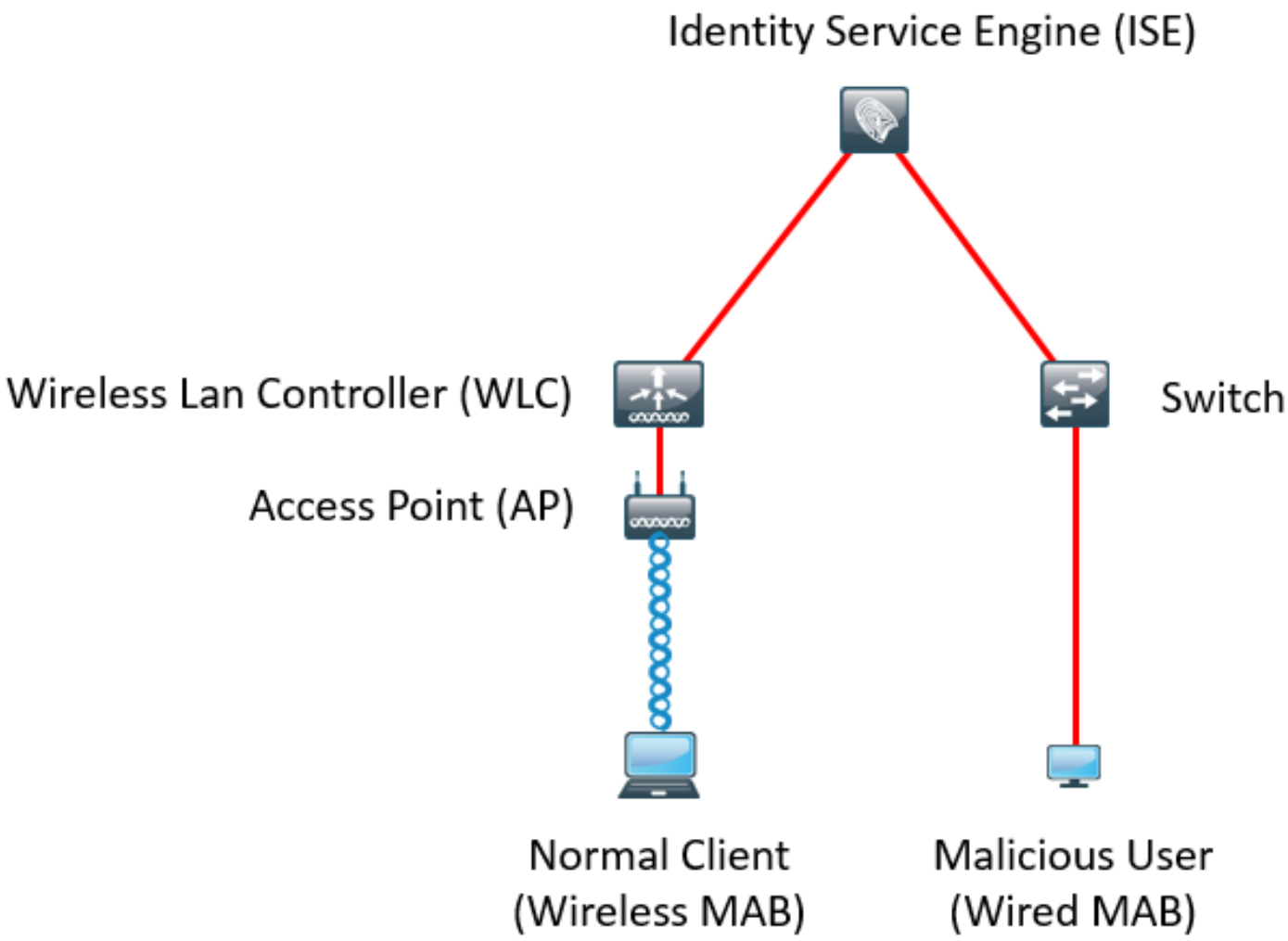
1. **NAS-Port-Type** - Определяет, изменился ли метод доступа этой оконечной точки. например, если тот же MAC-адрес для беспроводного Dot1x и визы-versa, который соединился через Проводной Dot1x использовался
2. **ID Класса DHCP** - Определяет, изменился ли тип клиента/поставщика оконечной точки.
3. **Операционная система -** Значительные изменения ОС, такие как Windows к iOS Apple.
4. **Политика оконечной точки -** Значительные изменения профиля. Например, отличие от Телефона или Принтера к ПК.

Как только ISE обнаруживает одно из упомянутых выше изменений, атрибут AnomalousBehaviour добавлен к оконечной точке и установлен в True. Это может использоваться позже в качестве условия в Политике авторизации для ограничения доступа для оконечной точки на будущих аутентификациях.

Если Осуществление настроено, ISE может передать CoA, как только изменение обнаружено, чтобы пройти повторную проверку подлинности или выполнить сильный удар порта для оконечной точки. Если в действительности, это может изолировать аномальную оконечную точку в зависимости от Политики авторизации, которая была настроена.

Настройка

Схема сети

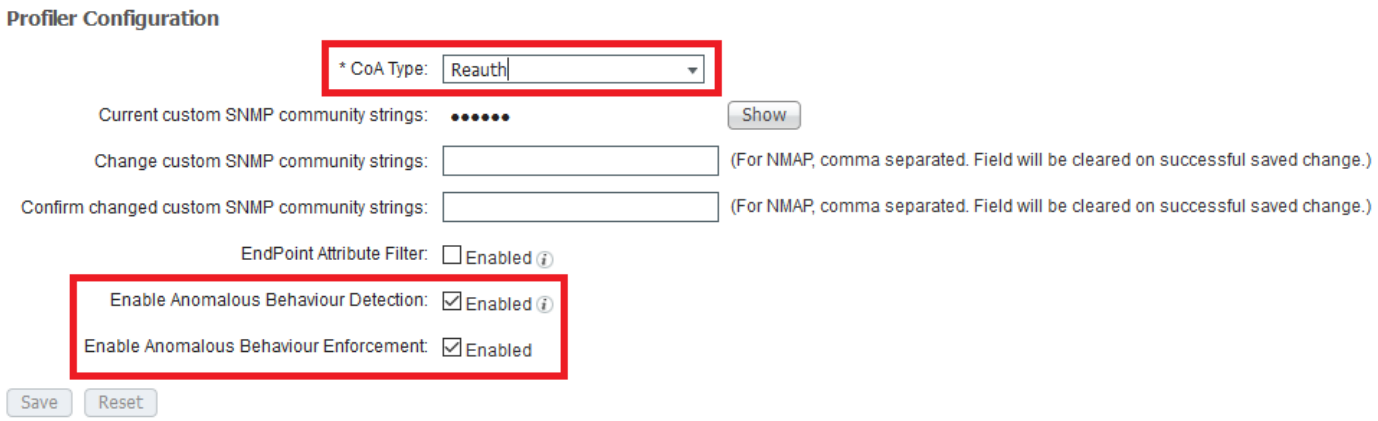


Конфигурации

Простой MAB и конфигурации AAA выполнены на коммутаторе и WLC. Для использования этой функции выполните эти действия:

Шаг 1. Включите аномальное обнаружение.

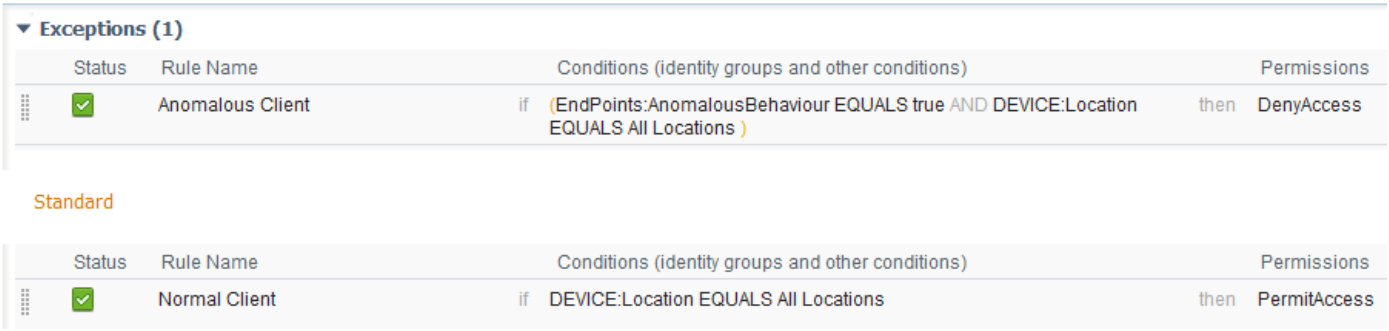
Перейдите к **администрированию> Система> Параметры настройки> Профилирование**.



Первый вариант позволяет ISE обнаруживать любое аномальное поведение, но никакой CoA не передается (Режим Только для видимости). Вторая опция позволяет ISE передавать CoA, как только аномальное поведение обнаружено (Режим Осуществления).

Шаг 2. Настройте Политику авторизации.

Настройте атрибут Anomlousbehaviour как условие в Политике авторизации, как показано в образе:

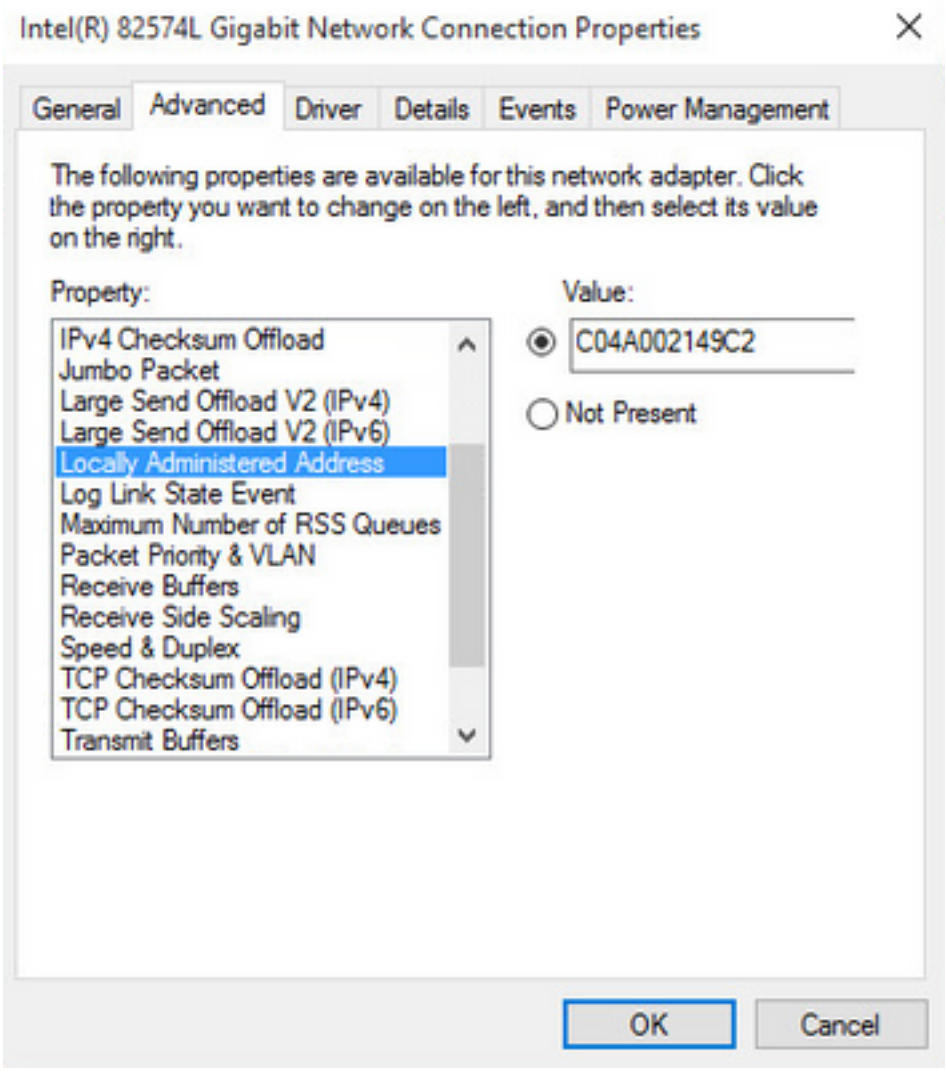


Проверка

Подключение с беспроводным адаптером. Используйте команду **ipconfig / все** для обнаружения MAC-адреса беспроводного адаптера, как показано в образе:

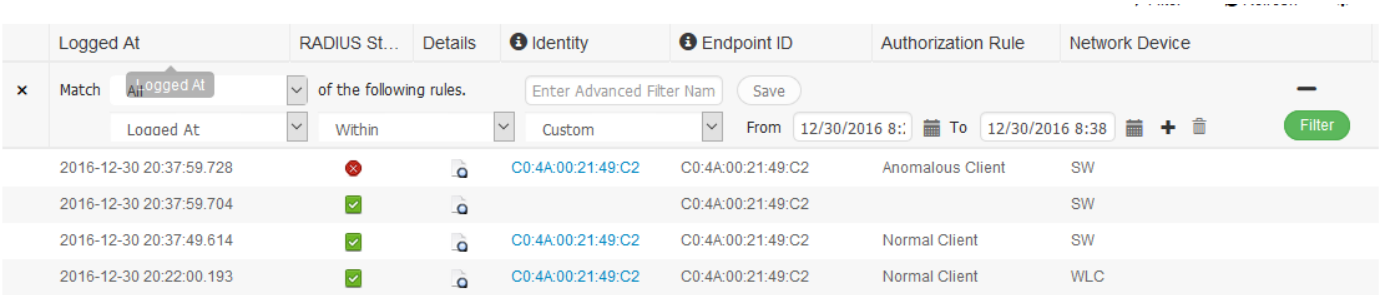
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : 802.11n USB Wireless LAN Card
   Physical Address. . . . . . . . . : C0-4A-00-21-49-C2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1c54:884a:33c0:bcf1%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.38(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, December 30, 2016 5:17:12 AM
   Lease Expires . . . . . . . . . . : Friday, December 30, 2016 6:17:12 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 46156288
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1F-F3-74-5F-C0-4A-00-21-49-C2
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Для моделирования злонамеренного пользователя можно имитировать MAC-адрес Адаптера ethernet для соответствия с MAC-адресом обычного пользователя.

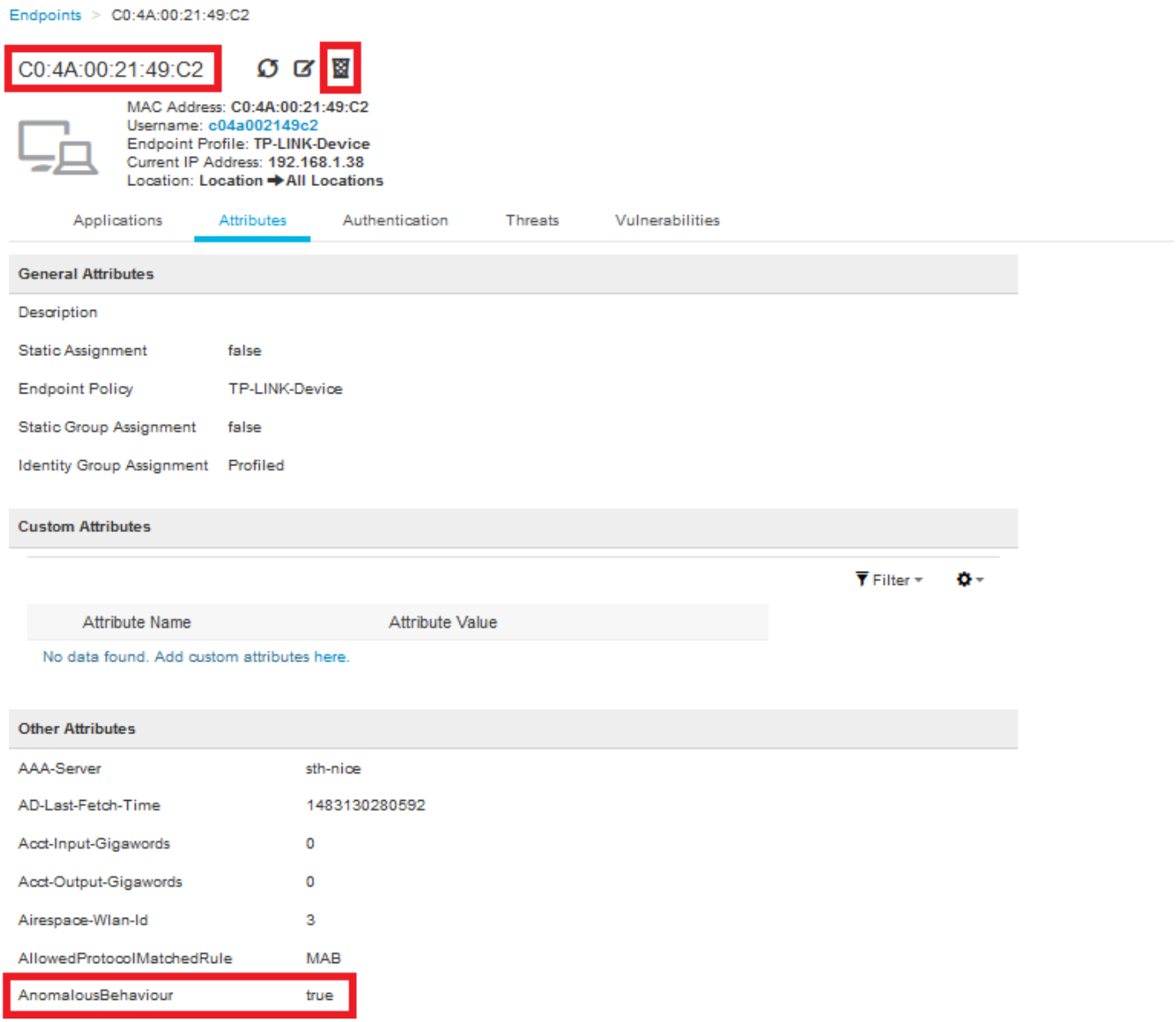


Как только Обычный пользователь соединяется, вы видите запись оконечной точки в базе данных. Впоследствии, подключения злонамеренного пользователя с помощью поддельного MAC-адреса.

Из отчётов вы видите первоначальное подключение от WLC. Впоследствии, подключения злонамеренного пользователя и 10 секунд спустя, CoA инициирован из-за обнаружения аномального клиента. Так как глобальный тип CoA установлен в **Reauth**, оконечная точка пытается соединиться снова. ISE уже установил атрибут AnomalousBehaviour в True, таким образом, ISE совпадает с первым правилом, и запретите пользователя.

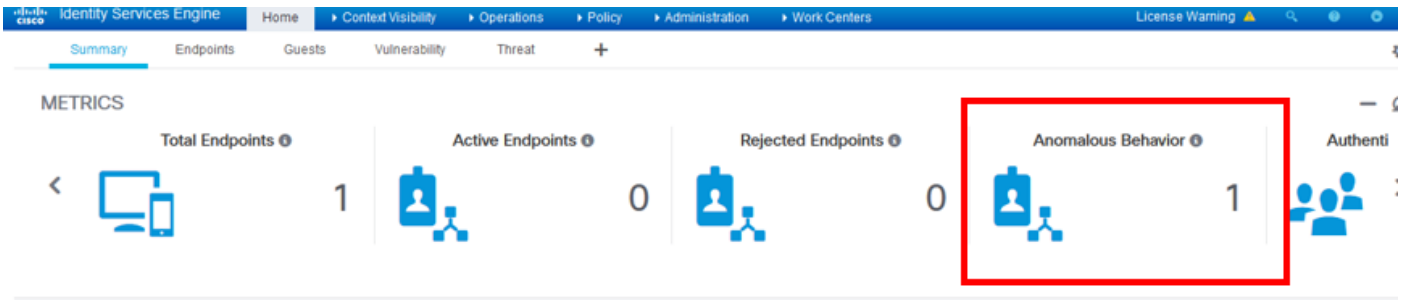


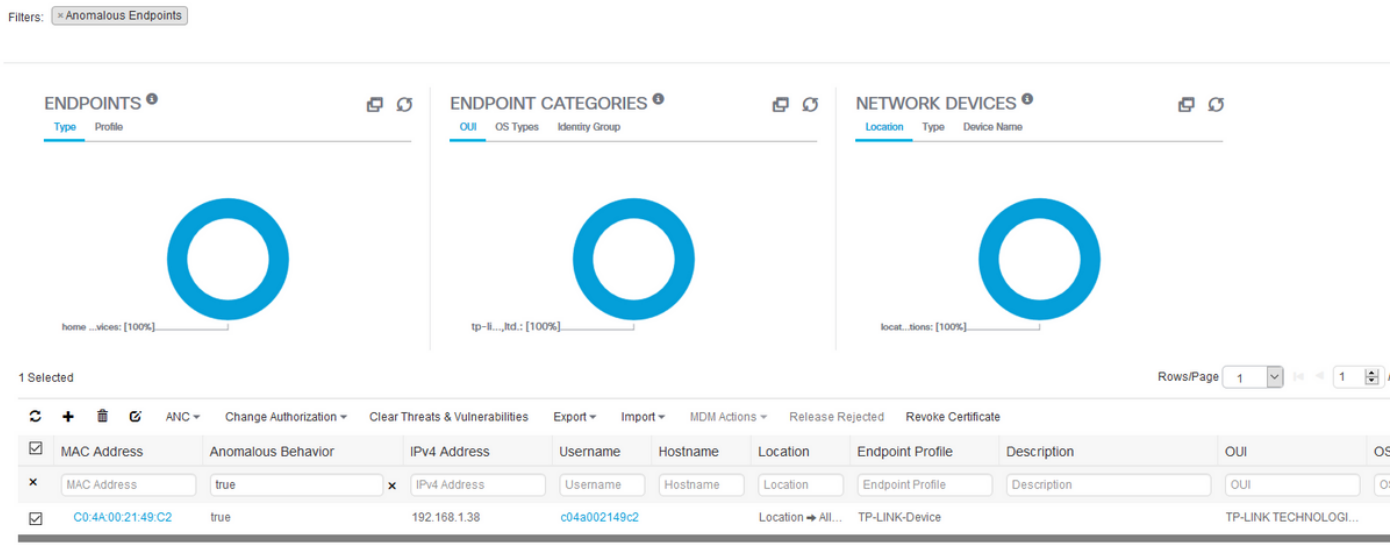
Как показано в образе, вы видите подробные данные под оконечной точкой во Вкладке Видимости Контекста:



Как вы можете видеть оконечная точка может быть удалена из базы данных для очистки этого атрибута.

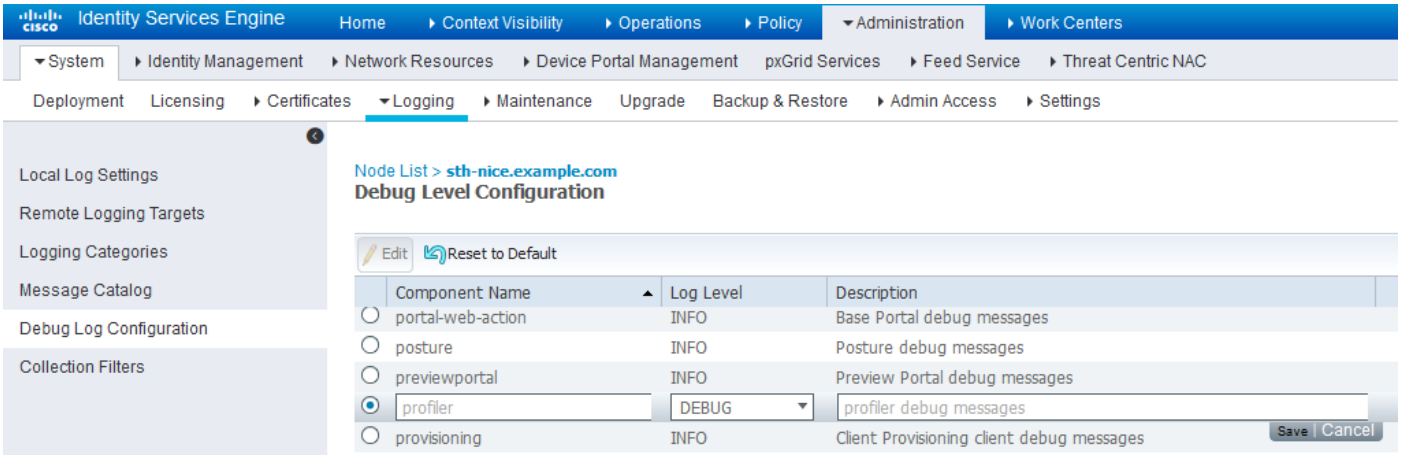
Как показано в образе, информационная панель включает новую вкладку для показа количества клиентов , показывающих это поведение:



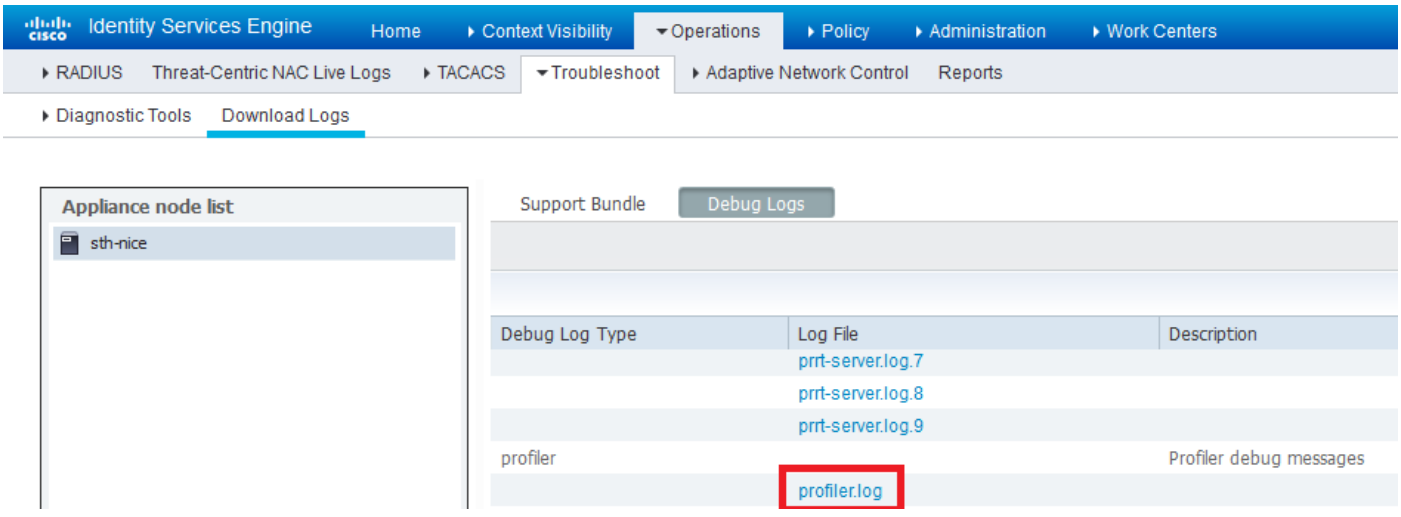


Устранение неполадок

Для устранения проблем включите отладку профилировщика, поскольку вы перешли к **администрированию> Система> Регистрация> Конфигурация Журнала Отладки**.



Для обнаружения ISE файлом **Profiler.log** перейдите к **Операциям> Журналы Загрузки> Журналы Отладки**, как показано в образе:



Эти журналы показывают некоторые фрагменты от файла **Profiling.log**. Как вы можете видеть ISE смог обнаружить, что оконечная точка с MAC-адресом C0:4A:00:21:49:C2

изменила метод доступа путем сравнения старых и новых значений атрибутов Port-type NAS. Это - радио, но изменено на Ethernet.

```
2016-12-30 20:37:43,874 DEBUG  [EndpointHandlerWorker-2-34-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:Profiling:- Classify hierarchy
C0:4A:00:21:49:C2
2016-12-30 20:37:43,874 DEBUG  [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2 2016-12-30 20:37:49,618
DEBUG [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Received
AttrsModifiedEvent in MACSpoofingEventHandler MAC: C0:4A:00:21:49:C2 2016-12-30 20:37:49,618
INFO [MACSpoofingEventHandler-52-thread-1][] com.cisco.profiler.api.MACSpoofingManager -
:ProfilerCollection:- Anomalous Behaviour Detected: C0:4A:00:21:49:C2 AttrName: NAS-Port-Type
Old Value: Wireless - IEEE 802.11 New Value: Ethernet 2016-12-30 20:37:49,620 DEBUG
[MACSpoofingEventHandler-52-thread-1][] cisco.profiler.infrastructure.cache.EndPointCache -
:ProfilerCollection:- Updating end point: mac - C0:4A:00:21:49:C2 2016-12-30 20:37:49,621 DEBUG
[MACSpoofingEventHandler-52-thread-1][] cisco.profiler.infrastructure.cache.EndPointCache -
:ProfilerCollection:- Reading significant attribute from DB for end point with mac
C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 DEBUG [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.EndpointPersistEventHandler -:ProfilerCollection:- Adding
to queue endpoint persist event for mac: C0:4A:00:21:49:C2
```

Поэтому ISE принимает меры, так как осуществление включено. Действие здесь должно передать CoA в зависимости от глобальной конфигурации в Копировальных упомянутых выше параметрах настройки. В нашем примере тип CoA установлен в Reauth, который позволяет ISE проходить повторную проверку подлинности оконечную точку и перепроверять правила, которые были настроены. На этот раз это совпадает с Аномальным клиентским правилом, и поэтому это запрещено.

```
2016-12-30 20:37:49,625 INFO   [MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Taking mac
spoofing enforcement action for mac: C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 INFO
[MACSpoofingEventHandler-52-thread-1][]
profiler.infrastructure.probemgr.event.MACSpoofingEventHandler -:ProfilerCollection:- Triggering
Delayed COA event. Should be triggered in 10 seconds 2016-12-30 20:37:49,625 DEBUG [CoAHandler-
40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received
CoAEvent notification for endpoint: C0:4A:00:21:49:C2 2016-12-30 20:37:49,625 DEBUG [CoAHandler-
40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Configured
Global CoA command type = Reauth 2016-12-30 20:37:49,626 DEBUG [CoAHandler-40-thread-1][]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Received
FirstTimeProfileCoAEvent for endpoint: C0:4A:00:21:49:C2 2016-12-30 20:37:49,626 DEBUG
[CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:-
Wait for endpoint: C0:4A:00:21:49:C2 to update - TTL: 1 2016-12-30 20:37:49,626 DEBUG
[CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:-
Setting timer for endpoint: C0:4A:00:21:49:C2 to: 10 [sec] 2016-12-30 20:37:49,626 DEBUG
[CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:-
Rescheduled event for endpoint: C0:4A:00:21:49:C2 to retry - next TTL: 0 2016-12-30 20:37:59,644
DEBUG [CoAHandler-40-thread-1][] cisco.profiler.infrastructure.profiling.CoAHandler -
:ProfilerCoA:- About to call CoA for nad IP: 10.62.148.106 for endpoint: C0:4A:00:21:49:C2 CoA
Command: Reauth 2016-12-30 20:37:59,645 DEBUG [CoAHandler-40-thread-1][]
cisco.profiler.infrastructure.profiling.CoAHandler -:ProfilerCoA:- Applying CoA-REAUTH by AAA
Server: 10.48.26.89 via Interface: 10.48.26.89 to NAD: 10.62.148.106
```

Дополнительные сведения

- Руководство по администрированию ISE 2.2